REMARKS

This is in response to the Office Action mailed on January 7, 08. Claims 1-35 are now pending in this application.

§102 Rejection of the Claims

Claims 1-8 and 13-31 were rejected under 35 USC § 102(e) as being anticipated by Grawrock et al. (hereinafter referred to as Grawrock) US Patent No. 2002/0080974 B2. Applicant respectfully traverses. To sustain a 35 USC § 102 rejection, each element of a rejected claim must be disclosed in the cited document as set forth in the Office Action.

Among the differences, claims 1 and 24 recite "generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value. Among the differences, claims 5 and 28 recite "generating a hash across the data using the ephemeral value as a key of the hash." Among the differences, claim 13 recites "a signature logic to retrieve at least part of the data from the storage medium and to generate a cryptographic hash across the at least part of the data with a cryptographic key having a value that is equal to the ephemeral value."

Grawrock does not disclose the use of an ephemeral value as a cryptographic key to generate a digital signature or hash. The system in Grawrock uses the ephemeral value for performing a reversible encryption of the data "the authorization secret" so that particular data (static markers) therein can be verified. See Grawrock at [0035]. In particular, the private key (EAPRK) is used to perform decryption of the encrypted data so that the static markers therein can be verified. Thus, the system in Grawrock relates to use of an ephemeral value as a cryptographic key to perform encryption/decryption of data.

> [T]he authorization secret may contain some static markers to allow the TPM to determine if decryption was successful. . . . The encrypted authorization secret is transmitted over a link to the TPM along with static markers and perhaps additional parameters necessary for creation of the entity (block 340). Upon receipt, the TPM decrypts the encrypted authorization secret using EAPRK and determines whether the decryption was successful through comparison of static markers for example (block 345). (emphasis added).

Grawrock at [0035].

In contrast, claims 1, 5, 13, 24 and 28 recite the use of a ephemeral value as the cryptographic key to generate a digital signature or hash. A digital signature or hash cannot be used to reproduce the decrypted data as required in the system in Grawrock. In contrast, the digital signature or hash is a value which is a representation of the data. However, the digital signature or hash cannot be used to reproduce the decrypted data. Rather, the digital signature or hash is used to authenticate the data. See Application at [0045]. Thus, Grawrock does not disclose the use of an ephemeral value as a cryptographic key to generate a digital signature or hash.

Because Grawrock does not disclose all of the claim limitations, Applicant respectfully submits that the rejection of claims 1, 5, 13, 24 and 28 under 35 USC § 102 has been overcome. Because claims 2-4, 6-8, 14-19, 25-27 and 29-31 depend from and further define claims 1, 5, 13, 24 and 28, respectively, Applicant respectfully submits that the rejection of claims 2-4, 6-8, 14-19, 25-27 and 29-31 under 35 USC § 102 has been overcome.

§103 Rejection of the Claims

Claims 9-12 and 32-35 were rejected under 35 USC § 103(a) as being unpatentable over Johnson, P.K. et al. (hereinafter referred to as Johnson) (WO 00/18162) in view of Grawrock et al. (hereinafter referred to as Grawrock) US Patent No. 2002/0080974 B2. Applicant respectfully traverses. Neither Johnson nor Grawrock (alone or in combination) discloses or suggests all of the claim limitations.

Among the differences, claims 9 and 32 recite "generating a second digital signature with a cryptographic key having a value that is equal to the random number." As noted by the Office, Johnson does not disclose this limitation. See Office Action at page 8. As noted above, Grawrock also does not disclose this limitation. Further, Applicant respectfully submits that there is no suggestion to modify Grawrock to generate a digital signature. In contrast, in order to be operative, Grawrock requires encryption/decryption of the data using a cryptographic key having a value that is equal to a random number such that the data can be reproduced so that the static markers can be verified. In contrast, claims 9 and 32 recite the generating of a digital

signature with such a cryptographic key. However, as noted above, the digital signature cannot be used to reproduce the encrypted data. Rather, the digital signature is used to authenticate.

Because neither Johnson nor Grawrock (alone or in combination) discloses or suggests all of the claim limitations, Applicant respectfully submits that the rejection of claims 9 and 32 under 35 USC § 103 has been overcome. Because claims 10-12 and 33-35 depend from and further define claims 9 and 32, respectively, Applicant respectfully submits that the rejection of claims 101-2 and 33-35 under 35 USC § 103 has been overcome.

RESERVATION OF RIGHTS

In the interest of clarity and brevity, Applicant may not have addressed every assertion made in the Office Action. Applicant's silence regarding any such assertion does not constitute any admission or acquiescence. Applicant reserves all rights not exercised in connection with this response, such as the right to challenge or rebut any tacit or explicit characterization of any reference or of any of the present claims, the right to challenge or rebut any asserted factual or legal basis of any of the rejections, the right to swear behind any cited reference such as provided under 37 C.F.R. § 1.131 or otherwise, or the right to assert co-ownership of any cited reference. Applicant does not admit that any of the cited references or any other references of record are relevant to the present claims, or that they constitute prior art. To the extent that any rejection or assertion is based upon the Examiner's personal knowledge, rather than any objective evidence of record as manifested by a cited prior art reference, Applicant timely objects to such reliance on Official Notice, and reserves all rights to request that the Examiner provide a reference or affidavit in support of such assertion, as required by MPEP § 2144.03. Applicant reserves all rights to pursue any cancelled claims in a subsequent patent application claiming the benefit of priority of the present patent application, and to request rejoinder of any withdrawn claim, as required by MPEP § 821.04.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 371-2103 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 371-2103

Date 4-7-08

By _____
Gregg A. Peacock
Reg. No. 45,001

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 7th day of April, 2008.

Dawn M Poole

Name

Dawn M. Poole

Signature